CONTENTS

Chapter 1 Introduction 4

1.1 Blockchain Architecture 4

1.2 Structure of a Block 5

1.3 Binary Merkle Tree 5

1.4 Transaction Lifecycle 6

Chapter 2 Review of Literature 8

2.1 Rationale 11

Chapter 3 Objectives of the Study 13

Chapter 4 Methodology 14

4.1 Research Procedure 14

4.2 Design Flow 15

4.3 Tools 16

4.3.1 Hyperledger 16

4.3.2 Ethereum 16

References 17

CHAPTER 1
INTRODUCTION

In 2008, Nakamoto the developer of crypto currency, Bitcoin introduced the concept of Blockchain technology. It is a mechanism originally developed to provide security to electronics transactions by making them immutable and ensuring their auditability. Blockchain describes method to reach consensus among unreliable participants. Normally, trusted third parties like banks or notary offices are responsible for validation, storage and security of transactions. But blockchain eliminates the requirement of mediator third parties since all the transactions are stored in blockchain ledger in a decentralized manner.

Blockchain that was first utilized for crypto currency, Bitcoin can be defined as a distributed, shared and append-only database. It is a type of distributed ledger or database that stores transactions or events in the form of blocks. New transactions are grouped together to form blocks. Each block may contain multiple transactions. This distributed database is replicated on each machine (nodes) participating in the network.

1.1 BLOCKCHAIN ARCHITECTURE

A blockchain consists of a network of nodes and a shared or replicated database among these nodes. All the participating nodes in the network can access these blocks, however none of them can delete or alter the data or transactions once stored in the blockchain. All the blocks containing transactions are connected in a chain using hash values. Each block contains the hash of the previous block in the chain connecting these blocks to the first block, known as genesis block. New blocks are added to the previous blocks using cryptographic hash functions like MD5 and SHA256. For example, Bitcoin uses SHA-256, cryptographic hashing algorithm, Litecoin uses Scrypt and Primecoin uses Cunningham chain as hash functions [1].

Cryptographic Hash Functions are highly secured one way function. Hash functions have some special properties making them highly secure. They are:

- Hash functions convert any size of data into a fixed size hash value.

- These are one way functions, i.e. the message digest obtained from hashing can't be used to obtain the message.
- No two messages can have the same hash value, even a small change in message results in a totally different hash.

1.2 Structure of a Block

Every block is having a header and a body. The header contains metadata like timestamp, previous hash, nonce (a random number used for cryptographic operations) etc. The size of the block can vary. The individual blocks in a blockchain are linked with each other using the hash values. Whenever, a new block is to be added to the blockchain, it calculates a new hash value which is generated using secure hash algorithm, SHA-256 [1]. Every block contains the hash of its previous block in its header [2] as shown in Figure 1. This creates a sequence of hashes linking blocks in a chain pointing to the first block in the chain, which is known as Genesis block [3]. If any changes are made in the content of block, the calculated hash value also changes. As the previous hash is included in the next block, so to make any changes to an existing block in the blockchain, it will require to change all the subsequent blocks. This provides the security and immutability to the blockchain transactions or contents.

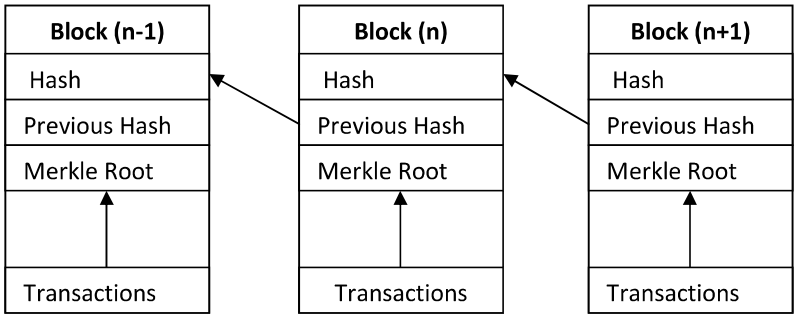


Figure 1: Blockchain Structure

1.3 Binary Merkle Tree

Each block comprises of one or more transactions grouped together. Blockchains use a binary Merkle Tree structure to store all these transactions. Merkle tree is also known as hash tree. In a Merkle tree, hashes of child's are combined to obtain hash of parent node [4]. All the leaf nodes in a Merkle tree are obtained by hash of the data or

transaction. That is all the leaf nodes contain hash of document or data. In a binary Merkle tree every non leaf node is a cryptographic hash obtained from combination of immediate Left and Right child node's hash.

Suppose there are 4 documents D1, D2, D3 and D4. Figure 2 shows a Binary Merkle Tree with 3 levels of cryptographic hash values; Root or Parent node, Level 1(L1) and Level 2(L2). L2 hashes are obtained by hashing all the documents individually, for example H00 is obtained from hashing document D1. Then at L1, H0 is obtained from combination of hash of D1 and D2 i.e. from H00 and H01. Same procedure is repeated for all other nodes. Lastly the final node root hash Hroot is obtained from combination of hash of L1. This parent node is known as root node or Merkle Root. In this way, Merkle root is made up of hash of all transactions in a block. This Merkle root is used to generate header of block comprising transactions.

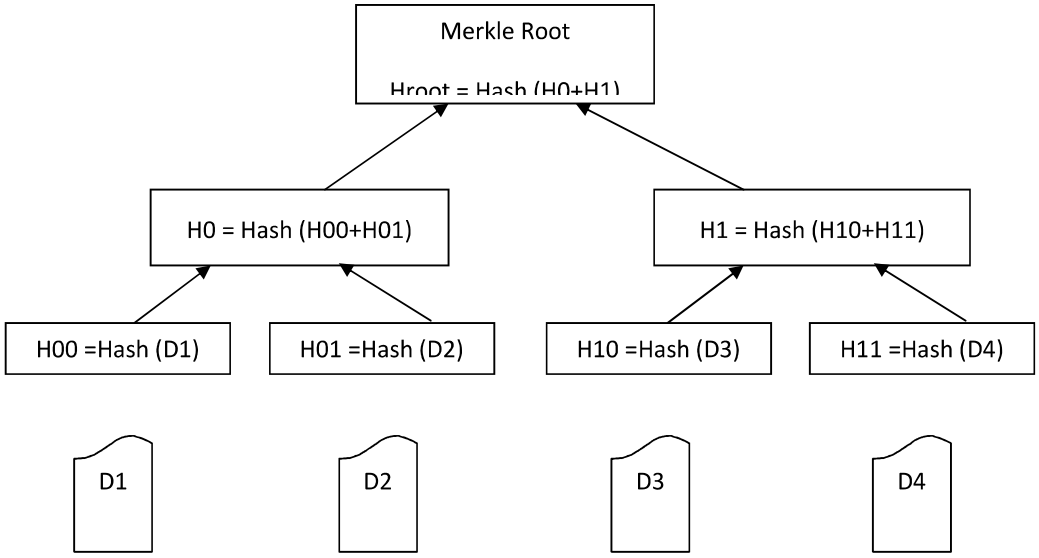


Figure 2: Binary Merkle Tree with 4 documents

Merkle tree gives us an advantage that by sharing only the Merkle root we can collectively secure multiple documents. If anyone tampers any document for example D1, then the hashes H00, H0 and Hroot all changes and can be easily detected. If Merkle root is shared on blockchain, it ensures no one alter any data or document.

1.4 TRANSACTION LIFECYCLE

Whenever a node creates a transaction, it signs the transaction using its own private key. Also it is encrypted using the public key of the receiver for whom this is meant,

so that only the node having the private key that matches the target public key can decrypt it. After that the node broadcasts it to all its neighbours. This makes the blockchain public while maintain privacy. Every node that receives the transaction relays it to its neighbours and so on. In this way the transaction is broadcasted so that it reaches to all the nodes in the network. When this transaction is received by a miner, it saves that transaction in order to include it in the next block. Miners are the peers in the network who validates the blocks in the transaction. Miners collect all the transactions over a time period and construct a new block. Mining procedure (depending on the protocol) is used to connect the newly constructed block to existing blockchain. To add a new block miners compete with each other [5]. Every miner obtains a hash after validating the new block against the Blockchain history (previous transactions). After calculating the hash, new block is added to the blockchain. Updated blockchain is then broadcasted in the network. Once a transaction is included in a block, and the block is included in the chain, it becomes public and immutable.

CHAPTER 2
REVIEW OF LITERATURE

Blockchain is the technology behind the digital crypto-currency, Bitcoin but it is not limited up to currency or finance. As the technology has great potential to provide security, it is being researched and used as a solution to make systems secure. Blockchain technology has a great potential to provide decentralized security and privacy. In 2016, Dorri et. al. proposed that special characteristics of blockchain technology like decentralization, immutability and auditability make it a potential platform to provide IoT device security. The decentralized nature of blockchain ensures scalability and robustness that avoids the risk of single point of failure [6].

In 2016, Chirstidis and Devetsikiotis described the potential of combining blockchain technology with IoT to automate the processes using smart contracts. By connecting the smart devices to the blockchain network as nodes, IoT devices can be controlled using smart contracts. Real-time data of the device status can be obtained by storing the information provided by smart devices on blockchain. And the devices can be made to transact among themselves automatically using smart contracts. By using a smart tracker on containers connected with Internet and installing blockchain in them, it is possible to revolutionize the supply chain industry [7]. Blockchain can be integrated with IoT to fulfil the security and privacy requirements for many application domains like smart homes, smart grids, health industry, supply chain, commodities, healthcare, digital identity, real estate, social networks and food industry. [8], [9], [10].

Blockchain and Internet of Things are finding great application in logistics particularly supply chain. Smart contracts are being developed based on Ethereum to connect and manage smart storage containers for logistics which have the sensors and are part of IoT network [11]. Blockchain architecture because of its strong consensus mechanism can be used in E-commerce to provide a trusted trading framework. Peer blockchain architecture can be used to support large number of high security transactions with lower latency [12].

In 2016, Azaria et. al. proposed that application of blockchain in biomedical domain. Health care is one of the most indispensable parts of life. Using blockchain, decentralized record management system can be provided to patients and doctors to maintain electronic medical records. The system will provide patients an easy and comprehensive access to their medical information stored in immutable ledgers [13]. Nowadays IoT based wearable devices are also available for health monitoring. Some remote patient monitoring facilities are also available. These technologies pose risk at patient's privacy and secure data transactions. In 2019, Vazirani et. al. Proposed that blockchain can provide a secure management of patient's electronic health records and medical conditions [14]. Blockchain can be involved to maintain the integrity, privacy and access control of electronic health records. In 2019, Drosatos and Kaldoudi proposed some interesting applications other than the health records, like clinical trials, medicine insurance and medicine supply chain [15].

In 2017, Rodrigues et. al. proposed a collaborative architecture using blockchain and smart contracts for DDoS mitigation across multiple domains. Usage of blockchain and smart contracts allows for the sharing of information in a fully distributed way. This property can be used to share attack information in an automated manner [16]. A new architecture is proposed by using smart contracts in blockchain for efficient DDoS mitigation techniques. It leverages the existing public and distributed infrastructure for advertising white or blacklisted IP addresses, for providing additional security to present DDoS defense system. By using the existing distributed infrastructure there is no need to build specialized registries or other distribution mechanisms.

In 2018, Shuling analyzed the concepts and uses of blockchain technology in smart city infrastructure [17]. Increasing internet connectivity exposes many confidential details comprising the security goals of CIA triad (Confidentiality, Integrity, and Availability). In 2018, Zhou et. al. proposed blockchain based smart home framework that can be utilized to detect and prevent security attacks like Distributed Denial of Service (DDOS) attack and linking attacks which endangers user's privacy [18].

In 2018, Poraghily et. Al. proposed benefits of distributed features of the blockchain technology for IoT devices. In Ethereum blockchain network the shared resources are

directly connected to the blockchain. These resources can be controlled by smart contracts. Pouraghily et. al. [19] presented the design guidelines for such IoT devices and the smart contracts controlling them. The proposed architecture can be implemented using Raspberry Pi and Ethereum testnet.

In 2018, Choi et. al. proposed that IoT devices can be securely controlled using smart contracts. The implementation of blockchain in IoT can provide authentication, non-repudiation and integrity without the involvement of any central authority. Smart contract in blockchains can prevent tempering of data from possible threats. The blockchain can be implemented as ethereum nodes on Raspberry Pi using node.js and web3 library. [20]

User authentication is very critical aspect for security and integrity of any web based security applications. Web based applications largely rely on centralized security approaches as they are easier to implement. But the centralized approach bears some security flaws like the risk of single point of failure. Blockchain technology can be used as a decentralized solution for access management in IoT networks. In 2017, Jansen presented a decentralized two-factor authentication mechanism for increasing the security [21].

In 2018, Novo proposed a blockchain based architecture for controlling rights and permissions in IoT based systems. The architecture follows complete distributed system for access control rights [22]. Blockchain technology can also be used to provide an access control on the data stored in the cloud. This decentralized ledger system provides immutable log of events and access management without the service provider intervention. Such a prototype system can be implemented on Ethernet platform using smart contracts [23]. Smart-contract based frameworks can be used for access control in IoT. Access control mechanism using smart contracts are trustworthy and distributed [24].

In 2018, Maesai et. al. proposed that access Control services can be implemented using smart contracts. Access Control policies can be executed as codes using smart contracts in blockchain. In addition Attribute Managers can also be implemented as smart contracts managed by blockchain. This makes the process completely distributed and automated execution using smart contract [25].

In 2018, Ouaddah et. al. proposed a framework FairAccess, for managing decentralized access control for IoT based on blockchain. This framework provides access management for constrained devices by using decentralized privacy preserving framework [26]. In 2018, Homoliak et. al. proposed a framework with two factor authentication for protection in case user's private key is stolen. It works in two stages and utilizes one time passwords created by using Merkle root, hash chains and pseudo random function [27].

In 2018, Lunardi et. al. proposed the concept of gateways that can be used to manage access to data and services in IoT based architectures. Gateways in IoT networks play an important role in controlling device communication. They can be used as decentralized access control solution for IoT. Raspberry Pi, Orange Pi and arduino are the conventional devices used in IoT networks. These devices can be configured to use cryptography and hashing algorithms such as SHA256, RSA and AES algorithms. Raspberry Pi 2 and Orange Pi Zero can be used as gateways and Arduino can be used as edge device to manage sensors and actuators due to its processing limitation. Different blockchain implementations like Ethereum and HyperLedger can be tested. In order to reduce the overhead, data from devices could be stored in a cloud environment [28].

2.1 RATIONALE

Centralized network architecture faces the following challenges:

- Single point of failure
- User has to trust third party for data handling and storage. Data stored on central servers has the risk of being deleted or tampered.
- User has limited control over the data stored in central servers. It can be used for analysis of personal information relating to health, social behaviours, purchasing preferences etc.

The involvement of central authority makes data vulnerable to attacks and misuse. User should have complete control over the ownership of own data like who has the right to access their data etc. Blockchain is decentralized in nature. It provides immutability and auditability to the data. The integration of blockchain with IoT can provide the data transparency. Blockchain can give the users opportunity to share

information and control the access to the data without intervention of central authority.

For online services securing the data and verifying the identity of users is a big challenge. Presently, online services are dependent on online service providers for identity management and authentication. These services rely on passwords stored on some central server. Emails and password credentials are easy to crack through hacking. Sometimes dual factor authentication is used for online authentication, but it relies on codes sent over SMS or other third party services like Gmail. Blockchain can eliminate the need of service provider for storing user credentials by making it decentralized.

With the rapid growth of portable insecure devices and increase in network traffic, attacks like Distributed Denial of Service (DDoS) are becoming a threat to online services. In DDoS attacks, malicious nodes flood the server or cloud with unnecessary requests or queries. This large amount of unnecessary traffic may result in crashing the server and denial of service to legitimate users. Such types of attacks are difficult to avoid as it is very difficult for the server to differentiate between actual and fake traffic. Blockchain can help in sharing the attack information in distributed manner and advertise the white and blacklist IP addresses.

CHAPTER 3
OBJECTIVES OF THE STUDY

The following objectives are identified based on the literature review:

1. Implementation of Blockchain based distributed architecture for enhancing security and privacy in peer-to-peer networks.
2. Comparative Analysis of Hyperledger (permissioned) and Ethereum (permissionless) blockchain networks and investigation of blockchain based solutions for different applications.
3. Investigation and analysis of collaborative DDoS attacks on distributed systems and design a blockchain based algorithm using smart contracts to mitigate DDoS attacks for securing distributed systems.
4. Design of a secure and efficient decentralized identity management technique for authentication and authorization of IoT devices connected in distributed network without involvement of any central authority.

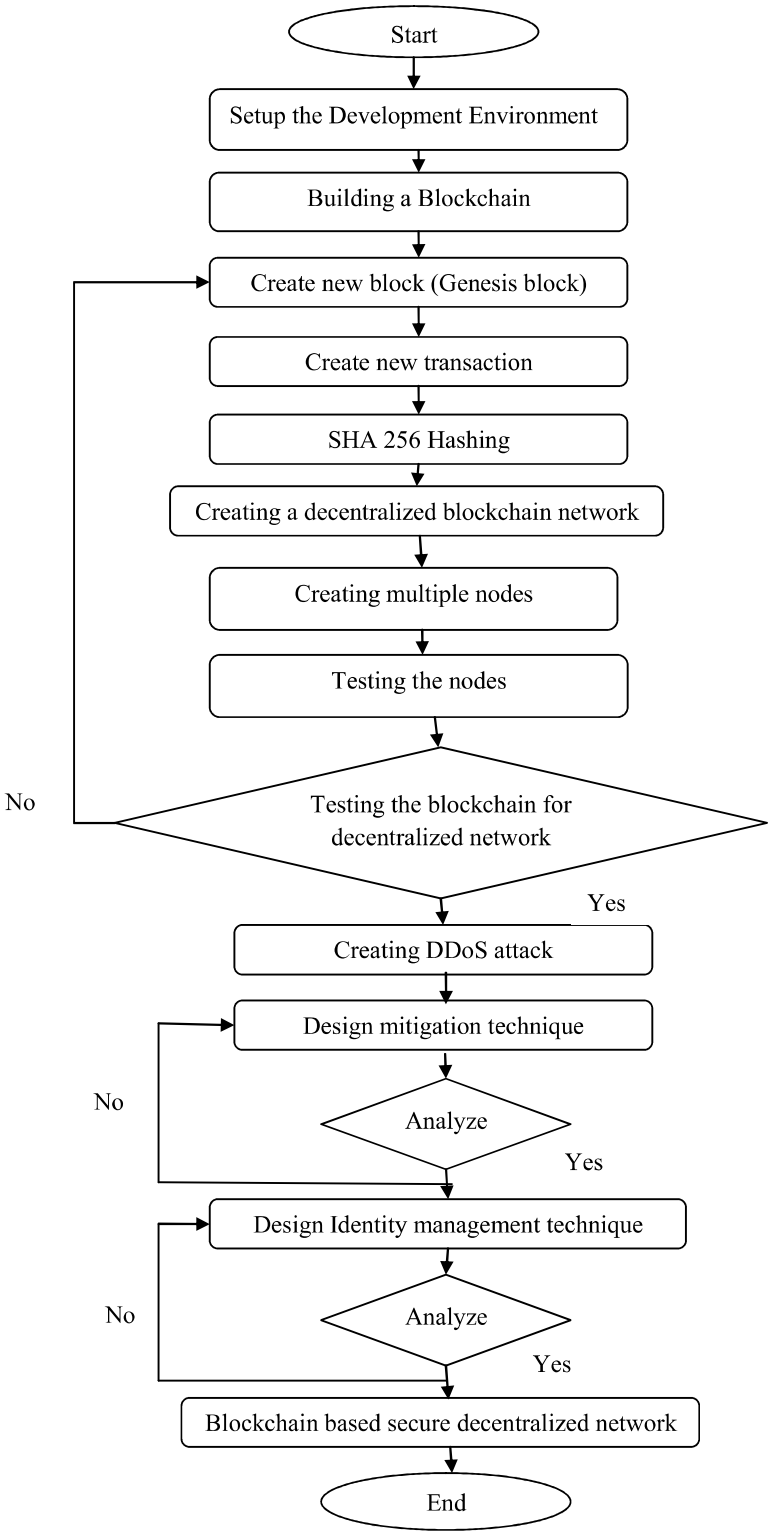
CHAPTER 4
METHODOLOGY

4.1 RESEARCH PROCEDURE

Following proposed research procedure will be followed for satisfactory fulfilment of objectives:

1. Analysis of blockchain technology and understand the difference between centralized and decentralized systems.
2. Analyze the benefits and applications of blockchain for achieving security, privacy and reliability in decentralized networks.
3. Analyze different platforms available for implementation of blockchain applications like Hyperledger and Ethereum.
4. Implement a distributed blockchain and identify the suitable simulation tool and products available for analysis of blockchain.
5. Develop a scenario in blockchain network, where situations, such as orphaned blocks and forks occur.
6. Analyze DDoS security threat on networks and design and propose a blockchain based DDoS mitigation technique.
7. Designing identity management scheme and analyzing it for enhancing security in distributed networks.

4.2 DESIGN FLOW



4.3 TOOLS

IBM Hyperledger and Ethereum Test Net will be studied in this research.

4.3.1 HYPERLEDGER

It is an open source collaboration started by Linux Foundation in December 2015, and IBM is one of the biggest contributors since 2017. It was created to advance the development of blockchain technology across industry. Its main aim is to develop open protocols and standards for blockchain.

4.3.2 ETHEREUM

It is a decentralized platform created for deployment of smart contracts, based on a blockchain. It also provides its own currency, Ether. Smart contracts used in Ethereum are computer codes that contains terms of agreements between untrusted parties to ensure trust and transparency between them.

REFERENCES

[1] Juan A Garay, Aggelos Kiayias, and Nikos Leonardos, "The Bitcoin Backbone Protocol: Analysis and Applications," *Advances in Cryptology - EUROCRYPT 2015*, vol. 2, pp. 281–310, 2015.

[2] Michael Crosby, Nachiappan, Pradan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman, "BlockChain Technology: Beyond Bitcoin," *Applied Innovation Review*, no. 2, pp. 1-16, 2016.

[3] Sachchidanand Singh and Nirmala Singh, "Blockchain: Future of Financial and Cyber Security," in *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, Noida, India, 2016, pp. 463-467.

[4] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *2017 IEEE 6th International Congress on Big Data*, 2017, pp. 557-564.

[5] D. Kraft, "Difficulty control for blockchain-based consensus systems," *Peer-to-Peer Networking and Applications*, vol. 9, no. 2, pp. 397–413, 2016.

[6] Ali Dorri, Salil S. Kanhere, Raja Jurdaky, and Praveen Gauravaram, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Kona, HI, 2017, pp. 618-623.

[7] Konstantinos Christidis and Michael Devetsikiotis, "Blockchains and Smart Contracts forthe Internet of Things," *IEEE Access Special Section on The Plethora of Research in Internet of Things (IoT)*, vol. 4, pp. 2292-2303, June 2016.

[8] Francesco Restuccia, Salvatore D'Oro, Salil S. Kanhere, Tommaso Melodia, and Sajal K. Das, "Blockchain for the Internet of Things: Present and Future," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 1-8, January 2018.

[9] Dennis Miller, "Blockchain and the Internet of Things in the Industrial Sector," *IT Professional Published by the IEEE Computer Society*, vol. 20, no. 3, pp. 15-18, May/June 2018.

[10] Muhammad Salek Ali et al., "Applications of Blockchains in the Internet of Things: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, pp. 1-41, 2018.

[11] Johannes Hinckeldeyn and Jochen Kreutzfeldt, "Developing a smart storage container for a Blockchain-based supply chain application," in *2018 Crypto Valley Conference on Blockchain Technology*, 2018, pp. 97-100.

[12] Wenlin Xie, Wei Zhou, Lanju Kong, Xiangdong Zhang, and Xinping Mi, "ETTF: A Trusted Trading Framework Using Blockchain in E-commerce," in *IEEE 22nd International Conference on Computer Supported Cooperative Work in Design*, 2018, pp. 612-617.

[13] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," *2016 2nd International Conference on Open and Big Data, IEEE Computer Society*, pp. 25-30, 2016.

[14] Anuraag A Vazirani, Odhran O'Donoghue, David Brindley, and Edward Meinert, "Implementing Blockchains for Efficient Health Care: Systematic Review," *Journal of Medical Internet Research*, vol. 21, no. 2, pp. 1-12, 2019.

[15] George Drosatos and Eleni Kaldoudi, "Blockchain Applications in the Biomedical Domain: A Scoping Review," *Computational and Structural Biotechnology Journal*, vol. 17, pp. 229–240, 2019.

[16] Bruno Rodrigues et al., "A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts," in *11th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2017*, Zurich, Switzerland, 2017, pp. 16–29.

[17] Li Shuling, "Application of Blockchain Technology in Smart City Infrastructure," in *IEEE International Conference on Smart Internet of Things*, 2018, pp. 276-282.

[18] Yiyun Zhou, Meng Han, Liyuan Liu, and Wang Yan, "Improving IoT Services in Smart-Home Using Blockchain Smart Contract," in *IEEE Confs. on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics*, 2018, pp. 81-87.

[19] Arman Pouraghily, Md Nazmul Islam, Sandip Kundu, and Tilman Wolf, "Poster Abstract: Privacy in Blockchain-Enabled IoT Devices," in *IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation*, 2018, pp. 292-293.

[20] Seong Seok Choi, Jin Wook Burm, Wonjin Sung, Ju Wook Jang, and Young Ju, "Blockchain-based Secure IoT Control Scheme," in *International Conference on Advances in Computing and Communication Engineering (ICACCE-2018)*, 2018, pp. 74-78.

[21] Marc Jansen, "About a Decentralized 2FA Mechanism," in *ICIW 2017 : The Twelfth International Conference on Internet and Web Applications and Services*, 2017, pp. 44-47.

[22] Oscar Novo, "Blockchain Meets IoT: an Architecture for Scalable Access Management in IoT," *Journal of Internet of Things Class Files*, vol. 14, no. 8, pp. 1-12, March 2018.

[23] Ilya Sukhodolskiy and Sergey Zapechnikov, "A Blockchain-Based Access Control System for Cloud Storage," in *IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, Moscow, 2018, pp. 1575-1578.

[24] Yuanyu Zhang, Shoji Kasahara, Yulong Shen, Xiaohong Jiang, and Jianxiong Wan, "Smart Contract-Based Access Control for the Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594-1605, April 2019.

[25] Damiano Di Francesco Maesai, Paolo Mor, and Paolo Mor, "Blockchain Based Access Control Services," in *2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics*, 2018, pp. 1379-1386.

[26] Aafaf Ouaddah, Anas Abou Elkalam, and Abdellah Ait Ouahman, "Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT," *Advances in Intelligent Systems and Computing*, pp. 523-533, 2018.

[27] Ivan Homoliak, Dominik Breitenbacher, Alexander Binder, and Pawel Szalachowski, "An Air-Gapped 2-Factor Authentication for Smart-Contract

Wallets," in *arXiv:1812.03598*, 2018.

[28] Roben Castagna Lunardi, Regio Antonio Michelin, Charles Varlei Neu, and Avelino Francisco Zorzo, "Distributed Access Control on IoT Ledger-based," in *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, IEEE Architecture*, Taipei, 2018, pp. 1-7.